(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/44995 A2

(51) International Patent Classification[7]: G06K

(21) International Application Number: PCT/FI01/01033

(22) International Filing Date:
27 November 2001 (27.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20002609 28 November 2000 (28.11.2000) FI

(71) Applicant *(for all designated States except US)*: **SETEC OY** [FI/FI]; Suometsäntie 1, FIN-01740 Vantaa (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **PAATERO, Lauri** [FI/FI]; Rikalantie 4, FIN-00970 Helsinki (FI).

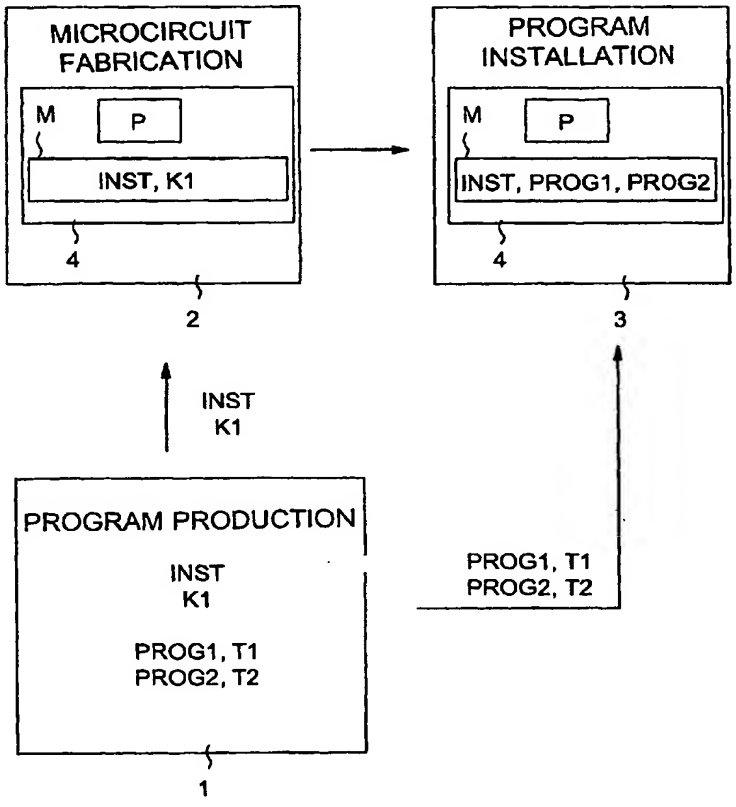
(74) Agent: **KOLSTER OY AB**; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EC, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent

[Continued on next page]

(54) Title: INSTALLATION OF PROGRAMS INTO MICROCIRCUIT



(57) Abstract: The present invention relates to a microcircuit comprising a memory (M) where a secret installation key (K1) is stored, means for receiving a program to be installed and a program-specific check value from external equipment, and a processor (P) for executing a predetermined installation program (INST) which checks on the basis of the secret installation key (K1) stored in the memory (M) and the program-specific check value (T1, T2) whether the program (PROG1, PROG2) to be installed is authentic and which installs said program if the check finds it authentic. To make sure that the secret installation key would not fall in the hands of outsiders even after installation, the microcircuit (4) is arranged to delete the secret installation key (K1) from the memory (M) prior to starting the program installed by the installation program (INST).

WO 02/44995 A2

(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INSTALLATION OF PROGRAMS INTO MICROCIRCUIT

The invention relates to installing programs into a microcircuit such that the microcircuit will be provided with only the programs the commissioner desires to be installed therein. The invention is well suited for applications where data security in installing the programs is of primary importance. In the following the invention will be described, by way of example, with reference to smart card manufacturing, even though it should be noted that the present invention can also be utilized in other applications.

Smart card manufacturing can roughly be divided into two different phases, the first of which is the fabrication of a microcircuit and the second is the installation of necessary programs. In smart card applications it is extremely important that the smart card manufacturer is fully aware of the programs that are installed in the microcircuit of the finished smart card. This is important, because if an outside aggressor has succeeded in loading a program of his own into the microcircuit of the smart card, the smart card serving as a pay card or an electronic identity card, for instance, may function in an unpredictable manner in certain situations, which causes considerable damage. Hence, the aim is to fabricate the smart card microcircuits such that only the correct programs can be installed into the microcircuit.

In prior art solutions, the microcircuit manufacturing process is divided into two phases, so that a microcircuit, in a memory of which a secret installation key and an installation program are stored, is manufactured in the first phase. For practical reasons, the fabrication of microcircuits is often commissioned to outside subcontractors, and the commissioner of the card hands over the installation key and installation program to be employed in the microcircuit fabrication to the subcontractor. Thus, the same secret installation key and installation program are used in a large number of microcircuits.

In the second phase of the microcircuit manufacture, the actual programs and microcircuit-specific secret keys are installed in the microcircuits. The installation of the programs requires an installation key stored in the memory of the microcircuit during fabrication. A check value, on the basis of which the installation program of the microcircuit can check that an authentic program is in question, is generated for each program to be installed by means of the installation key. The installation program of the microcircuit will install into the microcircuit only the programs that it is able to authenticate by means of the

installation key. If the installation program finds that the program to be installed is authentic, it allows the installation of the program into the microcircuit. The installation of the program(s) being completed, the installed program starts up and begins functioning in the microcircuit.

In order to maximize the security in a manufacturing process as described above, the secret installation key, by which the correct check value of the program can be generated, is at the disposal of only few persons. So, only these few selected persons can accept the installation of a specific program into a microcircuit by generating a program-specific check value for said program by means of the secret installation key at their disposal.

A drawback with the above-described prior art solution is that a person belonging to the manufacturer's own personnel may have created a program, intentionally or unintentionally, by means of which the secret installation key of the microcircuit can be read from the microcircuit, said program having started up on the microcircuit. Because the person concerned is an employee in the manufacturing organization, a program created by this person may obtain an authentic program check value from a person who has access to the necessary secret installation key. In this manner, the program gets a check value on the basis of which the installation program of the microcircuit will identify it as an authentic program, and hence, allow the installation and start up thereof in the microcircuit. A microcircuit of this kind, with a readable secret installation key, may cause considerable trouble, because an outsider, having received the secret installation key by reading it from the microcircuit, can create any suitable programs and generate correct check values for them with the secret installation key. The installation programs of new microcircuits to be fabricated will thus identify these programs as authentic and consequently allow the installation thereof into the microcircuits.

The object of the present invention is to solve the drawback associated with the above-described prior art solution and to provide a solution that improves data security in the fabrication of microcircuits. This is achieved with a method according to the invention for installing programs into a microcircuit, the method comprising storing a secret installation key in a microcircuit memory during fabrication, generating a program-specific check value for the programs to be installed with the secret installation key, checking the authenticity of each program to be installed in connection with program installation by means of the secret installation key stored in the microcircuit memory and the

program-specific check value, and allowing the program installation only if said program is found authentic on the basis of the check. The method according to the invention is characterized by deleting the secret installation key, stored in the microcircuit memory, upon completion of the program installation, and starting the installed programs in the microcircuit after deletion of the secret installation key.

The invention also relates to a microcircuit, which comprises a memory, where a secret installation key is stored, means for receiving a program to be installed and a program-specific check value from external equipment, and a processor for executing a predetermined installation program which checks on the basis of the secret key stored in the memory and the program-specific check value, whether the program to be installed is authentic and which installs said program if it is found authentic on the basis of the check value. The microcircuit according to the invention is characterized by being arranged to delete the secret installation key from the memory prior to starting the program installed by the installation program.

The invention is based on the idea that manufacturing of microcircuits and installation of programs become much more secure, when the secret installation key needed for the program installation is deleted from the microcircuit memory prior to the start up of the installed program(s). Thus, the secret installation key of the microcircuit cannot fall in the hands of an outsider, even though the microcircuit would be provided with a program that enables reading of the secret installation key from the microcircuit memory. This results from the fact that the secret installation key was erased from the microcircuit memory before the program enabling its reading started up. The most considerable advantage of the solution according to the invention is thus the improved data security, because not even a person within the organization of the commissioner can create a situation where the secret key of the microcircuit would be readable from the microcircuit.

In one preferred embodiment of the invention, the programs to be installed into the microcircuit are classified in predetermined classes, whereby a class code is defined for each program to be installed, which class code is checked in connection with installation when the authenticity of the program is to be verified and which is utilized in the installation of the program. This embodiment according to the invention helps to pre-empt such intentional or unintentional errors that may arise from the wrong program classification. For in-

stance, if a program designed for testing purposes is incorrectly classified as a production program and it is thereafter transferred to a microcircuit for installation, the installation program of the microcircuit attempts to install it the way the production programs should. Because the program actually is a test program, the installation fails.

The preferred embodiments of the method and the microcircuit according to the invention are disclosed in the attached dependent claims 2 to 3 and 5 to 6.

In the following, the invention will be described in greater detail by way of example, with reference to the attached drawings, wherein

Figure 1 is a flow chart of a first preferred embodiment of a method according to the invention;

Figure 2 illustrates a first preferred embodiment of a microcircuit according to the invention;

Figure 3 illustrates a second preferred embodiment of the microcircuit according to the invention; and

Figure 4 illustrates how secret keys are stored in a memory of the microcircuit.

Figure 1 is a flow chart of a first preferred embodiment of a method according to the invention. The flow chart of Figure 1 can be utilized in installing programs into a microcircuit of a smart card, for instance.

In block A, an installation key is stored in the microcircuit in connection with fabrication. The same installation key is stored in the memory of a plurality of microcircuits in connection with fabrication.

In block B, a program-specific check value is generated for each program intended for installation into the microcircuit. The program-specific check value can be generated by an algorithm that computes a specific check value on the basis a program code and a secret installation key. Thus, the check value and the program code will form a pair, whose authenticity can be verified by means of the installation key.

In block C, the produced program and its check value are fed to the microcircuit. The memory of the microcircuit contains the same algorithm (part of the installation program) and the same secret installation key, by which the check value is generated in block B. Thus, the installation program of the microcircuit is able to check the authenticity of the program to be installed, i.e. the program is authentic if the result of the computational operation carried out

on the basis the secret key of the installation program and the program code matches with the check value.

If the microcircuit finds in block D that the program is not authentic, the installation program of the microcircuit interrupts the program installation by proceeding to block F. But if the program is authentic, the processor of the microcircuit executes the installation in accordance with installation program.

In block F, the microcircuit checks if there still are other programs to be installed. If not, it deletes the secret installation key from its memory in block G. Thereafter, the microcircuit starts the installed programs in block H.

Because the starting of the installed programs does not take place until in block H, after deletion of the secret installation key in block G, it is possible to pre-empt a situation where any one of the installed programs would enable reading the secret installation key from the microcircuit memory. This is not possible in the method according to the flow chart of Figure 1, because the secret installation key will no longer be in the microcircuit memory when the installed program starts up.

Figure 2 illustrates a first preferred embodiment of a microcircuit according to the invention. Figure 2 shows three separate production phases 1 to 3 of the microcircuit 4. This division can be utilized in the production of microcircuits intended for smart cards, when it is extremely important that only the correct programs will be installed into the microcircuit so that its operation would be fully predictable at all times. For instance, when smart cards are manufactured, the division can be such that a subcontractor manufactures the microcircuits, the commissioner of the microcircuits produces the necessary programs and secret keys, and the programs and the secret keys are installed into the microcircuits either by the commissioner or a third party.

The program production takes place in phase 1. In the case of Figure 2, it is assumed that programs PROG1 and PROG2 are to be installed into the microcircuits to be produced. However, it is not desired that these programs be handed over to production phase 2, where the actual fabrication of the microcircuit takes place. If the programs to be installed were handed over to the production phase 2, very high attention should be paid to the security in the production phase 2 so as to make sure that no outsider would have a chance to tamper the programs to be installed. Instead, from the program production it is possible to hand over an installation program INST and a secret installation key K1 to the production phase 2. These are stored in the memory

M of the microcircuits in connection with the mechanical microcircuit fabrication. When the microcircuit 4 leaves the production phase 2, it comprises at least a processor P and one or more memories M, where the necessary program(s) is/are stored in order to make it possible for the microcircuit to receive other data later on, such as programs and secret keys.

When the microcircuit 4 fabrication is completed and the installation program INST and the secret installation key K1 are stored in its memory M, the microcircuit is transferred to the production phase 3 where the programs PROG1 and PROG2 will be installed. To make this possible, the microcircuit is attached with pins (not shown in the figure) therein to external equipment, such as a computer peripheral. In order that the commissioner of the microcircuit could be sure that inappropriate programs are not installed, intentionally or unintentionally, in the microcircuit in the production phase 3, the installation program INST delivered from the program production to the microcircuit fabrication is selected such that it installs into the microcircuit only programs that are authentic on the basis of the authentication carried out with the secret installation key K1.

The authentication is made possible, when a check value T1 is computed for the program PROG1 in the program production by utilizing a predetermined algorithm, the program code PROG1 and the secret installation key K1. Correspondingly, a check value T2 is computed for the program code PROG2 by utilizing the secret installation key K1. The algorithm by which the check values are computed forms part of the installation program INST, and consequently it also exists in the memory of the microcircuit 4, for the microcircuit to be able to make the corresponding computational operation. In addition to the programs PROG1 and PROG2, also their check values T1 and T2 are thus forwarded from the production phase 1 to the production phase 3, i.e. to the program installation.

The check values T1 and T2 are applied with the programs PROG1 and PROG2 into the microcircuit through its input. The processor of the microcircuit 4 then carries out authentication by means of the algorithm included in the installation program INST, in which authentication it checks with the secret installation key K1 if the check values are correct. If the check values are correct, the installation program INST of the microcircuit installs the programs PROG1 and PROG2 into the microcircuit. When the installation is completed, the installation program deletes the secret installation key K1 from the memory

M of the microcircuit. Thereafter, the installation program starts the installed programs and ceases to function.

Figure 3 illustrates a second preferred embodiment of the microcircuit according to the invention. The embodiment of Figure 3 corresponds to great extent with that of Figure 2, and therefore the embodiment of Figure 3 will be described in the following primarily in so far as it differs from the embodiment of Figure 2.

The embodiment of Figure 3 employs program classification into different levels. For instance, three different levels can be employed:

1) production level programs, which have to be protected in such a manner that an outside aggressor is not able to get any data from the programs or the microcircuit in any way whatsoever,

2) clients' test level programs, which permit the clients to test their own programs and codes. For instance, in the case of a smart card, a typical client could be a bank whose data processing department should be able to test how the programs of their own production function in the microcircuit. Hence, the clients' test level programs are such that provide limited access to the information stored in the memory of the microcircuit.

3) manufacturer's test level programs, which permit the manufacturer to test how the microcircuits function. The manufacturer's test level programs thus provide unlimited access to the information stored in the memory of the microcircuit.

A class code LEVEL, which indicates the level of the program in question, is defined for the programs provided by the program production. When a check value is generated for a finished program PROG1 by means of the secret installation key K1, an algorithm is used which also utilizes the class code, in addition to the program code and the installation key. Correspondingly, the installation program INST' utilizes the same algorithm which takes into account the class code when checking the authenticity of the program prior to installation. In the embodiment of Figure 3, the programs PROG1 and PROG2 to be installed, their class codes LEVEL1 and LEVEL2 and the check values T1 and T2 of the programs are thus forwarded from the production phase 1 to the production phase 3.

The installation program INST' stored into the microcircuit 4 during fabrication is made such that it processes programs of different levels differently. In other words, if for some reason a test level program is classified as a

production level program on the basis of the class code, the installation of this program fails, because the installation program INST' subjects it to operations during installation, which lead in a successful installation if a test program is concerned, but in a failure if a production level program is concerned. This can be implemented, for instance, such that the installation program performs class-code-dependent computational operations in connection with the installation, whereby the computational operations proceed to a correct final result (successful installation) for the program to be installed, only, if said program is given a correct class code.

Figure 4 illustrates the storing of secret keys in the memory of the microcircuit. The storing of the secret keys as described in Figure 4 can be utilized in the embodiments of both Figure 2 and Figure 3. In other words, in addition to what is described as stored in the memory of the microcircuit in connection with Figures 2 and 3, it is also possible to store secret keys as indicated in Figure 4.

In the example of Figure 4 the storing of secret keys is described assuming that the storing of programs takes place according to the embodiment of Figure 2. Hence, this example does not employ class codes of the programs. In the case of Figure 4 there are two keys to be stored, i.e. A1 and A2. In connection with secret key production, the keys are encoded, whereby they can be transferred to the production phase 3 without that any outsider finds out the secret keys. The secret keys are encoded with a code key K2 which is computed by a predetermined coding algorithm by utilizing a random number RND and the secret installation key K1. When the code key K2 is computed, the keys A1 and A2 are encoded such that the encoded keys A1' and A2' are obtained. These encoded keys A1' and A2' and the random number RND are forwarded to the production phase 3, where they will be applied to the microcircuit in connection with the program installation.

In the case of Figure 4, the microcircuit installation program INST" is employed, which includes the above-mentioned coding algorithm, whereby the processor of the microcircuit can compute the code key K2 by means of the secret installation key K1 and the random number RND received in the production phase 3. By means of this code key the installation program of the microcircuit can decode the encoded keys A1' and A2' such that the secret keys A1 and A2 are stored in the memory of the microcircuit.

It should be understood that the above description and the relating figures are only intended to illustrate the present invention. It is apparent to a person skilled in the art that the invention can be varied and modified in a variety of ways without deviating from the scope and spirit of the invention disclosed in the accompanying claims.

CLAIMS

1. A method for installing programs into a microcircuit, the method comprising

storing a secret installation key in a microcircuit memory during fabrication,

generating a program-specific check value for the programs to be installed with the secret installation key,

checking the authenticity of each program to be installed in connection with program installation by means of the secret installation key stored in the microcircuit memory and the program-specific check value, and

allowing the program installation only if said program is found authentic on the basis of the check, **characterized** by

deleting the secret installation key, stored in the microcircuit memory, upon completion of the program installation, and

starting the installed programs on the microcircuit after deletion of the secret installation key.

2. A method as claimed in claim 1, **characterized** by

classifying the programs to be installed into the microcircuit into predetermined classes and defining for each program to be installed a class code indicating the class of the program,

generating said program-specific check value by an algorithm, which takes into account the class code of the program, in addition to the secret key and the program, and

checking the authenticity of each program to be installed in connection with installation by means of the secret key stored in the memory of the microcircuit and the program class code applied to the microcircuit, and

installing the program class-code-dependently, if the program is found authentic on the basis of the check.

3. A method as claimed in claim 2 or 3, **characterized** in that for storing the secret keys into the memory of the microcircuit, the method comprises

computing a code key by a coding algorithm which utilizes the secret installation key and a random number,

encoding the secret keys to be stored with the computed code key,

applying the encoded secret keys and said random number to the microcircuit, and

computing the code key by means of the secret installation key stored in the memory of the microcircuit, the random number and said coding algorithm, and decoding the encoded secret keys with the computed code key and storing the secret keys into the memory.

4. A microcircuit comprising

a memory (M) where a secret installation key (K1) is stored,

means for receiving a program to be installed and a program-specific check value from external equipment, and

a processor (P) for executing a predetermined installation program (INST, INST', INST") which checks on the basis of the secret installation key (K1) stored in the memory (M) and the program-specific check value (T1, T2), whether the program (PROG1, PROG2) to be installed is authentic, and which installs said program if it is found authentic on the basis of the check, **characterized** in that the microcircuit (4) is arranged to delete the secret installation key (K1) from the memory (M) prior to starting the program installed by the installation program (INST, INST', INST").

5. A microcircuit as claimed in claim 4, **characterized** in that

the microcircuit (4) is arranged to receive a class code (LEVEL1, LEVEL2) of the program to be installed together with the program (PROG1, PROG2) and the program-specific check value (T1, T2), and that

the microcircuit (4) is arranged to utilize the program-specific class code (LEVEL1, LEVEL2) in checking the authenticity of the program (PROG1, PROG2) to be installed and to install the program class-code-dependently if the program is found authentic on the basis of the check.

6. A microcircuit as claimed in claim 4 or 5, **characterized** in that

the microcircuit (4) comprises means for receiving encoded secret keys (A1', A2') and a random number (RND) from external equipment, and that

the microcircuit (4) is arranged to compute a code key by means of a predetermined coding algorithm, a secret installation key (K1) and said random (RND), and to decode the encoded secret keys (A1', A2') with said code key and to store the secret keys (A1, A2) into the memory (M).

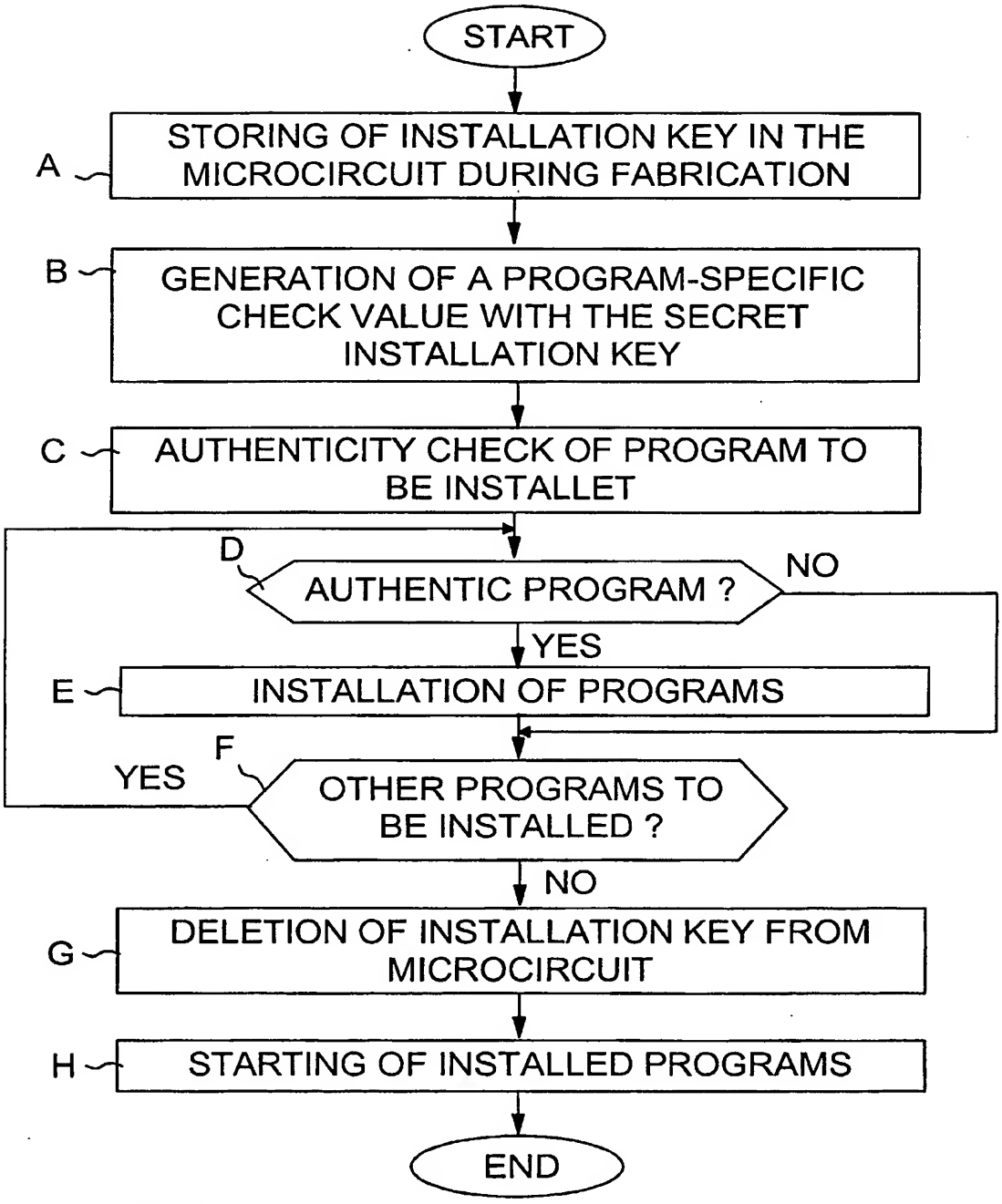

START
A
STORING OF INSTALLATION KEY IN THE MICROCIRCUIT DURING FABRICATION
B
GENERATION OF A PROGRAM-SPECIFIC CHECK VALUE WITH THE SECRET INSTALLATION KEY
C
AUTHENTICITY CHECK OF PROGRAM TO BE INSTALLET
D
AUTHENTIC PROGRAM ?
NO
YES
E
INSTALLATION OF PROGRAMS
F
YES
OTHER PROGRAMS TO BE INSTALLED ?
NO
G
DELETION OF INSTALLATION KEY FROM MICROCIRCUIT
H
STARTING OF INSTALLED PROGRAMS
END

FIG. 1

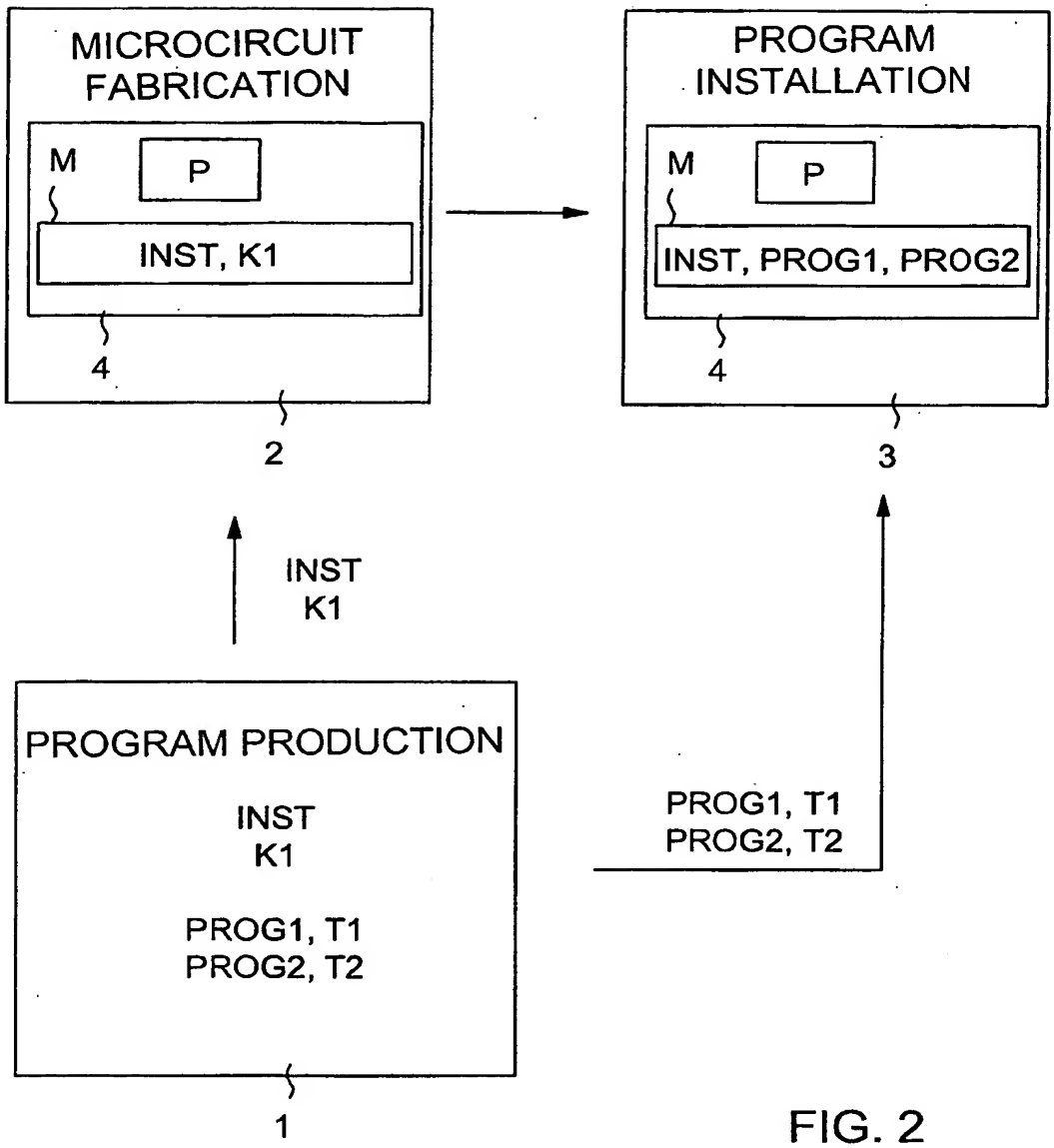

MICROCIRCUIT FABRICATION
M
P
INST, K1
4
2
PROGRAM INSTALLATION
M
P
INST, PROG1, PROG2
4
3
INST
K1
PROGRAM PRODUCTION
INST
K1
PROG1, T1
PROG2, T2
1
PROG1, T1
PROG2, T2

FIG. 2

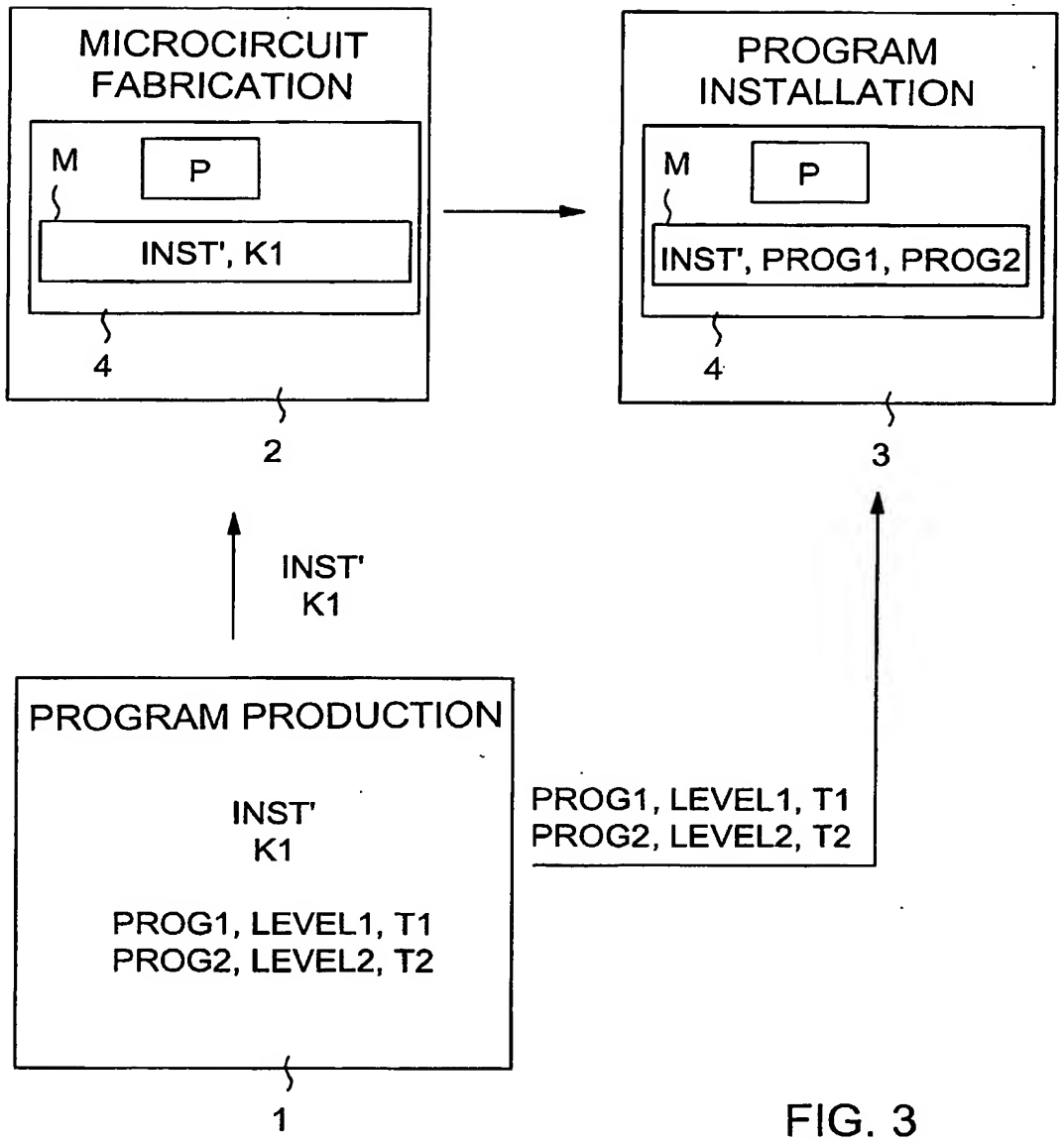

MICROCIRCUIT FABRICATION
M
P
INST', K1
4
2
PROGRAM INSTALLATION
M
P
INST', PROG1, PROG2
4
3
INST'
K1
PROGRAM PRODUCTION
INST'
K1
PROG1, LEVEL1, T1
PROG2, LEVEL2, T2
PROG1, LEVEL1, T1
PROG2, LEVEL2, T2
1

FIG. 3

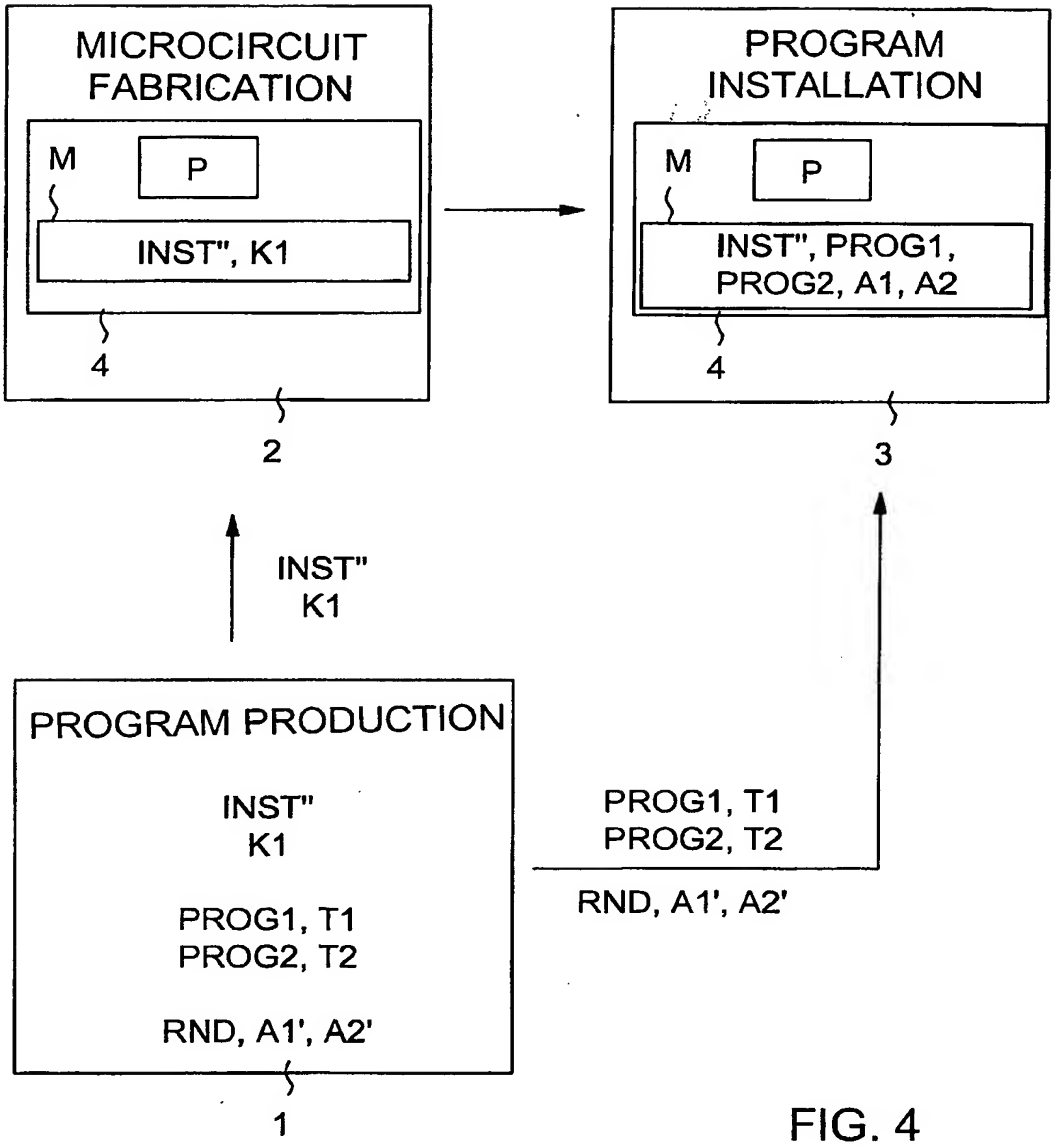

MICROCIRCUIT FABRICATION
M
P
INST", K1
4
2
PROGRAM INSTALLATION
M
P
INST", PROG1, PROG2, A1, A2
4
3
INST" K1
PROGRAM PRODUCTION
INST" K1
PROG1, T1
PROG2, T2
RND, A1', A2'
1
PROG1, T1
PROG2, T2
RND, A1', A2'

FIG. 4